

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
ASHEVILLE DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
APPLE ID  
**COURTNEYMILLIARD@YAHOO.COM**  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE, INC.

Case No. 1:18mc33

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael Gregory, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since 2012. In my current capacity, I am assigned to investigate federal crimes against children, to include: international parental kidnapping, child abductions, sexual exploitation of children, domestic trafficking of children/prostitution, child sex tourism and national sex offender registry violations. I have received extensive training in investigations as a New Agent Trainee at the FBI Academy in Quantico, Virginia, as well as follow on training as it relates to my current assignment. As a federal

agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence and contraband (in the form of child pornography) of violations of 18 U.S.C. § 2251, Sexual exploitation of children, as described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

6. The Federal Bureau of Investigation is investigating the production of child pornography by William Richard Hilliard JR (Hilliard), a resident of Cleveland County, North Carolina. Hilliard was arrested on June 11, 2018 by Myrtle Beach Police Department (MBPD) for surreptitiously filming several girls showering on his yacht.

7. On June 10, 2018, Child Victim 7 (CV7), made a report with MBPD in reference to finding an iPad filming her showering while on Hilliard's yacht. CV7 babysits for Hilliard and as a graduation

gift, he took CV7, her mother and several of her friends on his yacht in Myrtle Beach, South Carolina. While CV7 was showering, she saw an iPad sticking out of Hilliard's bag that was positioned towards the shower. After CV7 inspected the iPad, she noticed it had been recording her for approximately 15 minutes. She stopped the video and went through the camera roll, noting other videos were on the iPad of the other seven (7) girls on the yacht. Along with those videos, CV7 observed there were videos of other females (of age and underage) taking showers.

8. CV7 deleted the videos on the iPad of the girls on the boat and developed a ruse to be brought into the harbor by Hilliard. After docking, CV7 and her mother made a report with MBPD.

9. On June 10, 2018, Detective Angel Walker, MBPD interviewed CV7 and the other girls that had been on the yacht. The seven (7) other girls told Detective Walker they had taken showers between Bird Island and Restaurant Row. CV7's mother told Detective Walker that Hilliard is her 4th cousin and he had been acting weird while they were all on the yacht. He would get her to steer the boat while he went and checked on the bathroom after every time one of the girls finished showering.

10. On June 11, 2018, Detective Walker interviewed Hilliard at the jail which was recorded. After advising him of his rights, Hilliard admitted to recording CV7 and the other girls on the yacht. He knows CV7 and her mother as they are distant cousins of his as well as CV7 babysits for him. He recorded them because he knew they would be naked in the shower. He advised Detective Walker he has been recording females for about the past two (2) years and that he sometimes pleasures himself after watching them. He also admitted to recording videos underneath a door. He said he has never sold any of the videos he made for profit. Of the girls recorded on his yacht, he acknowledged the youngest was 14 or 15 years of age.

11. Detective Walker obtained a state arrest warrant for Hilliard for violation of South Carolina 16-17-0470(B), sex/voyeurism and arrested him on June 11, 2018.

12. A state search warrant for Hilliard's yacht, described as a Cruiser's Yacht 460 Express (hull ID US-CRSSDA01D607) was obtained on June 11, 2018 and executed the same day. Detective S. Thackray, MBPD, seized several items to include two (2) laptops, SD memory cards, iPhone, iPod and a flash drive. Prior to executing the search warrant, Detective Thackray spoke with CV7 who pointed out where the shower was located on the yacht. She advised she was told to shower in Hilliard's room and that it never had a shower door attached because it was broken. Detective Thackray also discovered a shower door under a bench seat in the main room of the boat. MBPD obtained additional state search warrants for the items that were seized from the yacht.

13. The iPad that was found by CV7 which had recorded her and the other girls on the yacht, was processed by MBPD following a state search warrant. The Apple ID associated with the iPad was courtneymhilliard@yahoo.com.

14. On June 11, 2018, Cleveland County Sheriff's Office (CCSO) was made aware of Hilliard's arrest and of the suspicion he had filmed females at his residence, 2742 Clineland Road, Cherryville, North Carolina 28021, which is in Cleveland County. On June 12, 2018, CV7's mother was quoted in the Shelby Star, "The mother also said Hilliard secretly recorded video of baby sitters at the house in Cherryville." Detective Jessica Hamilton, CCSO, contacted CV7's mother the same day who told her after CV7 found the iPad recordings, she went through the iPad and found other recordings. Other recordings took place in Hilliard's daughter's bathroom at his residence in Cleveland County. CV7's mother was unable to provide further information but provided CV7's phone number to Detective Hamilton.

15. Detective Hamilton contacted CV7 the same day. CV7 said after she went through the recordings, she found a recording that took place in Hilliard's daughter's bathroom. CV7 was able to

describe the bathroom and knows the room from babysitting at his house for the past two (2) years. The recording she observed was of Child Victim 5 (CV5), who is of age, in the bathroom naked. CV7 knows CV5 as they both babysit for Hilliard.

16. On June 12, 2018, CCSO executed a search warrant at Hilliard's residence in Cleveland County. Several items were seized during the search warrant including but not limited to video cameras, cell phones, SD cards and DVDs. Investigators discovered the door to Hilliard's bathroom door, where CV7 had observed the recording of CV5, had tool marks at the bottom. The tool marks were rough but appeared to have been made for the sole purpose of putting a recording device under the door. No other tool marks like those were located in the residence and based on the upkeep of the rest of the residence, the tool marks did not seem to be "normal" wear and tear.

17. Investigators with CCSO reviewed the evidence seized from Hilliard's residence. Videos of various females showering or in the bathroom were located. Videos of Hilliard and Child Victim 3 (CV3) engaging in the course of sexual acts were also located. The acts included oral sex and masturbation.

18. Other videos were located that were of Hilliard watching the videos he recorded. The videos were of girls in the shower of Hilliard's yacht, along with vaginal sex, oral sex, digital penetration and females undressing in the bathroom. Detective Derek Shaffer, CCSO, advised of the videos that had been reviewed, it appeared there were approximately 30 victims that had been surreptitiously recorded and of those about 12-15 were underage.

19. On June 26, 2018, Detectives Hamilton and Shaffer contacted CV3 by phone and advised her of the videos that were located at Hilliard's residence. CV3, who is in her mid 20s, said when she was between 14-16 years of age, Hilliard paid her \$1500 total to have sex and let him video. The sexual acts

occurred while Hilliard was living at 404 Farris Drive, Cherryville, North Carolina which is in Gaston County. CV3 said she only knew of one (1) video Hilliard recorded and that was of her performing oral sex; she didn't think he recorded them having vaginal sex. She also remembered another incident that occurred when she was on his yacht. She had been intoxicated and he took videos of her while she was in the shower. CV3 said a lot of the incidents happened on his yacht while it was docked on Lake Wylie.

20. On June 27, 2018, Detectives Hamilton and Shaffer spoke to Courtney Hilliard (Courtney), wife of Hilliard. Courtney advised her family utilized her Apple ID (courtneymhilliard@yahoo.com) for all of their Apple devices.

21. Based on my training and experience and the training and experience of others with whom I have worked, there is probable cause to believe content stored on behalf and information associated with Apple ID courtneymhilliard@yahoo.com contain relevant and material information the ongoing criminal investigation, including but not limited to 1) picture and video files of underage females either engaging in sexual acts or naked and displayed in a lewd and lascivious manner; 2) messages or documentation specifying Hilliard's location(s); 3) IP address login information that may be helpful in identifying Hilliard's location(s) at various dates and times and 4) information that may reveal other relevant electronic communication accounts associated with the production of child pornography.

### **INFORMATION REGARDING APPLE ID AND iCloud<sup>1</sup>**

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and "iCloud: How Can I Use iCloud?," available at <https://support.apple.com/kb/PH26502>.

22. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

23. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and

share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

24. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

25. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent



by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

26. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

27. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

28. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM

card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

29. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

30. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records

described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

31. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

32. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

33. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

34. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

35. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

### **REQUEST FOR SEALING**

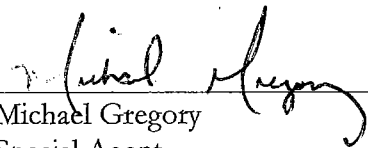
39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

### **REQUEST FOR NON-DISCLOSURE**

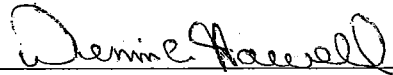
40. I further request that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Apple be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant until further order of the Court. Such an order is justified because notification of the existence of this warrant would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

WHEREFORE, it is respectfully requested that the Court grant the attached Order directing Apple not to disclose the existence of the warrant or the application except to the extent necessary to carry out the Order.

Respectfully submitted,

  
\_\_\_\_\_  
Michael Gregory  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on October 3, 2018

  
\_\_\_\_\_  
HONORABLE DENNIS L. HOWELL  
UNITED STATES MAGISTRATE JUDGE

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to information associated with courtneymhilliard@yahoo.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber



Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within up to 14 days of service of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2251, Sexual exploitation of children involving William Richard Hilliard JR, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence of violations relating to 18 U.S.C. § 2251 as described in Paragraphs 6-21 of the Affidavit.
- b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.